


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)
Search: The ACM Digital Library The Guide

endorsement certificate public key private key manufacturer hash



Searching within **The Guide** for: endorsement certificate public key private key manufacturer hash OR digest signature (start a new search)

Found 7 of 1,327,510

REFINE YOUR SEARCH
▼ Refine by Keywords

endorsement certificate



Discovered Terms

▼ Refine by People

Names

Institutions

Authors

▼ Refine by Publications

Publication Year

Publication Names

ACM Publications

All Publications

Content Formats

Publishers

▼ Refine by Conferences

Sponsors

Events

Proceeding Series

ADVANCED SEARCH

FEEDBACK

Please provide us with feedback

Found 7 of 1,327,510

Search Results
Related Journals
Related Magazines
Related SIGs
Rel...

Results 1 - 7 of 7

 Sort by in

1 Internet Security Glossary

R. Shirey

May 2000 Internet Security Glossary

Publisher: RFC Editor

 Full text available: [Tkt](#) (489.29 KB) Additional Information: [full citation](#), abstract, cited by

Bibliometrics: Downloads (6 Weeks): 12, Downloads (12 Months): 114, Citation Count: 1

This Glossary (191 pages of definitions and 13 pages of references) provides abbr explanations, and recommendations for use of information system security termin is to improve the comprehensibility of writing that deals with ...

2 On-board credentials with open provisioning

Kari Koistinen, Jan-Erik Ekberg, N. Asokan, Aarne Rantala

 March 2009 **ASIACCS '09: Proceedings of the 4th International Symposium on Infor and Communications Security**
Publisher: ACM

 Full text available: [Pdf](#) (1.17 MB) Additional Information: [full citation](#), abstract, references, in

Bibliometrics: Downloads (6 Weeks): 11, Downloads (12 Months): 33, Citation Count: 0

Securely storing and using credentials is critical for ensuring the security of many distributed applications. Existing approaches to address this problem fall short. Us passwords are flexible and cheap, but they suffer from bad ...

Keywords: credentials, provisioning protocols, secure hardware, trusted computi

3 Analysis and design of a hardware/software trusted platform module for embe

Najwa Aaraj, Anand Raghunathan, Niraj K. Jha

 December 2008 **Transactions on Embedded Computing Systems (TECS)**, Volume

Publisher: ACM

 Full text available: [Pdf](#) (1.13 MB) Additional Information: [full citation](#), abstract, references, in

Bibliometrics: Downloads (6 Weeks): 54, Downloads (12 Months): 374, Citation Count: 0

Trusted platforms have been proposed as a promising approach to enhance the se purpose computing systems. However, for many resource-constrained embedded and cost overheads of a separate Trusted Platform Module (TPM) ...

Keywords: Custom instructions, embedded systems, multiprocessor systems

4 Energy and execution time analysis of a software-based trusted platform mod

Najwa Aaraj, Anand Raghunathan, Srivaths Rayi, Niraj K. Jha

April 2007 **DATE '07:** Proceedings of the conference on Design, automation and test
Publisher: EDA Consortium

Full text available: Pdf (838.82 KB) Additional Information: [full citation, abstract, references](#)

Bibliometrics: Downloads (6 Weeks): 11, Downloads (12 Months): 113, Citation Count: 0

Trusted platforms have been proposed as a promising approach to enhance the se purpose computing systems. However, for many resource-constrained embedded and cost overheads of a separate Trusted Platform Module (TPM) ...

5 The advent of trusted computing: implications for digital forensics

Mike Burmester, Judie Muiholland

April 2006 **SAC '06:** Proceedings of the 2006 ACM symposium on Applied computing

Publisher: ACM

Full text available: Pdf (137.02 KB) Additional Information: [full citation, abstract, references, in](#)

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 114, Citation Count: 1

The release of computer hardware devices based on "trusted computing" technolo paradigm shift that will have profound implications for digital forensics. In this pa the contours of a trusted environment in order to establish ...

Keywords: cybercrime, data recovery, encryption, file systems, forensics, specific computing

6 Communications of the ACM: Volume 51 Issue 4

April 2008 Communications of the ACM

Publisher: ACM

Full text available: Digital Edition, Pdf (4.24 MB) Additional Information: [full citation](#)

Bibliometrics: Downloads (6 Weeks): 189, Downloads (12 Months): 2189, Citation Count

7 Communications of the ACM: Volume 51 Issue 7

July 2008 Communications of the ACM

Publisher: ACM

Full text available: Digital Edition, Pdf (6.54 MB) Additional Information: [full citation](#)

Bibliometrics: Downloads (6 Weeks): 3440, Downloads (12 Months): 6437, Citation Cour

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2009 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player